REMARKS

The Applicants and the undersigned thank Examiner Jackson for her careful review of this application. Claims 1-25 have been rejected. Upon entry of this amendment, Claims 1-25 are pending in this application.

The independent claims are Claims 1, 12, 13, 16, 19, 21, and 25. Consideration of the present application is respectfully requested in light of the above amendments to the application and in view of the following remarks.

Claim Rejections under 35 U.S.C. § 103

The Examiner rejected Claims 1-25 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,434,615 to Dinh et al (hereinafter the "Dinh" reference) in view of U.S. Patent No. 6,584,454 to Hummel, Jr. et al. (hereinafter the "Hummel" reference). The Applicants respectfully offer remarks to traverse these pending rejections.

Independent Claim 1

The rejection of Claim 1 is respectfully traversed. It is respectfully submitted that the Dinh and Hummel references fail to describe, teach, or suggest the combination of (1) completing a vulnerability assessment of the workstation to identify security vulnerabilities that would compromise the secure operation of the workstation on the computer network; (2) generating workstation security credentials based on the vulnerability assessment, the workstation security credentials comprising one of integrity information describing whether the workstation has been compromised, and security posture information describing the workstation's potential for compromise; (3) comparing the workstation security credentials to a workstation security policy to determine whether the workstation should be granted access to the network service; and (4) authorizing access to the network service by the workstation if the workstation security credentials satisfy the workstation security policy, otherwise denying access to the network service by the workstation, as recited in amended Claim 1.

The Dinh reference describes a controlling computer system 120 for performing remote system administration upon a stand alone computer system 110. The controlling

computer system 120 accesses the stand alone computer system 110 through a communications network using a remote communication protocol 130. See Figure 1 of Dinh reproduced below.

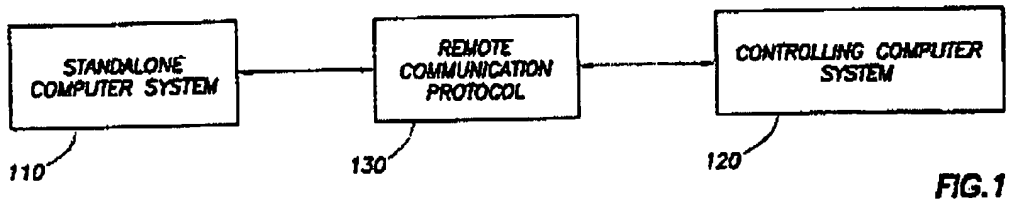


FIG. 1

After establishing a connection with the stand alone computer system 110, a preexisting diagnostic application on the stand alone computer system 110 is initiated using the established communication between the controlling computer system 120 and the stand alone computer system 110. See Dinh reference, column 2, lines 13-24.

The Dinh reference explains that the controlling computer system 120 will perform an overview status check on the remote stand alone computer system 110. Such a status will yield information such as the remote stand alone computer's processor type, the total memory in the remote stand alone computer system 110, and peripheral devices that are interfaced with the remote stand alone computer system 110. The Dinh reference further explains that the controlling computer system 120 will be able to display a screen that is substantially similar to the screen that would be displayed if a local diagnostic application were executed locally on the remote stand alone computer system 110. See Dinh reference, column 4, line 59 through column 5, line 2.

One of ordinary skill in the art recognizes that the remote diagnostic system 120 described by the Dinh reference does not provide any teaching of controlling access to a network service in connection with generating workstation security credentials based on the vulnerability assessment, wherein the workstation security credentials comprise one of integrity information describing whether the workstation has been compromised, and security posture information describing the workstation's potential for compromise, as recited in amended Claim 1. Dinh only describes a computer diagnostic system that does not address any security aspects whatsoever. In other words, one of ordinary skill in the art recognizes that the diagnostic information reviewed by the Dinh reference does not relate in any way to security vulnerabilities or security credentials.

To address authenticating a workstation requesting a network service, generating workstation security credentials, and completing a vulnerability assessment of the workstation, as recited in Claim 1, the Examiner referred the Applicants to column 7, lines 1-35 of the Dinh reference. This portion of the Dinh reference describes steps 430 through 450 as illustrated in Figure 4 of the Dinh reference. Figure 4 of the Dinh reference is reproduced below:

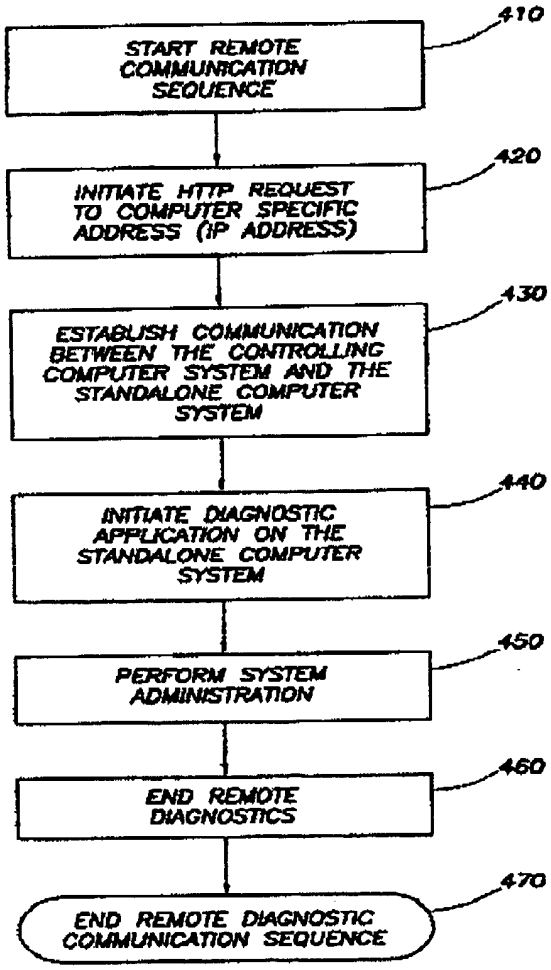


FIG.4

The Dinh reference explains that in step 430 communication is established between the controlling computer system 110 and the stand alone computer system 120 using the remote communication protocol 130. Next in step 440, the controlling

computer system 110 sends requests to a diagnostic application, such as Compaq Diagnostics®, running the stand alone computer system 120 to gather hardware and software information and to perform diagnostic tests. See Dinh reference, column 7, lines 30-34 and lines 55-57.

In step 450, the remote control computer system 120 performs system administration on the stand alone computer system 110. The system administration tasks performed on the stand alone computer system 110 include inspection of the hardware and software, status checks, hardware tests, and asset management. See Dinh reference column 7, lines 58-64.

The steps described above as illustrated in Figure 4 of the Dinh reference do not show completing a vulnerability assessment of the workstation to identify security vulnerabilities that would compromise the secure operation of the workstation on the computer network. These steps of the Dinh reference also do not show generating workstation security credentials based on the vulnerability assessment, as alleged by the Examiner. Further, the Dinh reference does not provide any teaching of authorizing access to a network service based on workstation security credentials comprising one of integrity information describing whether the workstation has been compromised, and security posture information describing the workstation's potential for compromise, as recited in amended Claim 1.

The Applicants remind the Examiner that for a rejection based upon 35 U.S.C. § 102, MPEP § 2131 (8th Ed., Rev. 2, May 2004) states:

> TO ANTICIPATE A CLAIM, THE REFERENCE MUST TEACH EVERY ELEMENT OF THE CLAIM...The identical invention must be shown in as complete detail as is contained in the claim. Richardson v. Suzuki Motor Co., 9 USPQ 2d 1913, 1920 (Fed. Cir. 1989)."

The Applicants submit that the Examiner has not shown the identical invention in as complete detail as is contained in amended independent Claim 1. Because the Dinh reference does not teach any aspects of computer security, the Applicants submit that this reference fails to teach numerous elements recited in independent Claim 1 and therefore, the Dinh reference fails to anticipate amended independent Claim 1.

The Examiner admits that the Dinh reference fails to provide any teaching of an log-in page or access denied page. As noted above, the Dinh reference does not pertain to computer security and therefore, log-in pages or access denied pages would never be described in a diagnostic system such as the Dinh reference. To make up for these deficiencies, the Examiner relies upon the Hummel reference.

The Hummel reference describes a method and system for delivering protected software applications 128 to remote systems 104 from a central service facility 110. Delivery of the protected software applications 128 is managed on the basis of the level of security clearance and on the basis of community membership of the remote system user. See Figure 5 of the Hummel reference reproduced below.

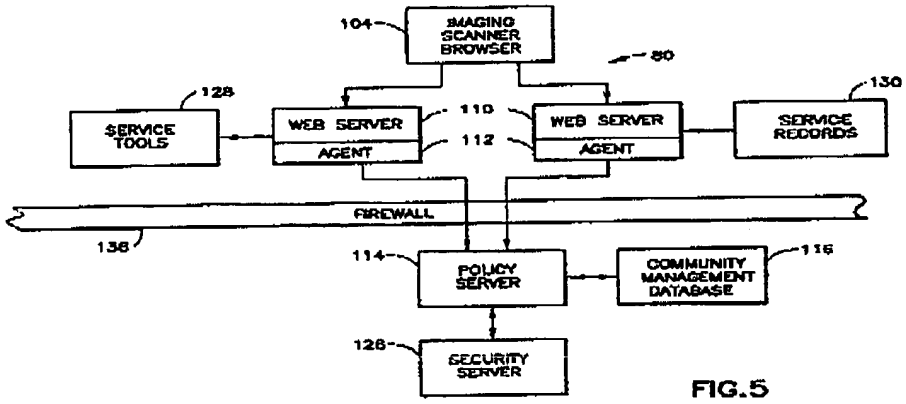


FIG.5

Remote systems 104 of the Hummel reference typically include magnetic resonance imaging (MRI) systems, computerized tomography (CT) systems, or ultrasound imaging systems. The system of the Hummel reference is designed to allow a field service engineer to use a browser running on a remote system, such as an MRI scanner 104, to access webservers 110 over the Internet 80. When the field service engineer provides either a one or two-factor security clearance to the webservers 110, the agents 112 will check with the policy server 114 and security server 126 to determine if the field service engineer's security clearance is valid.

The policy server 114 accesses a community management database 116 that stores access rights for remote system users. If the field service engineer's security clearance is valid, then the engineer will have access to files and applications in the service tools 128 for updating the MRI from its browser 104. See Hummel reference, column 8, lines 1-68.

One of ordinary skill in the art recognizes that the Hummel reference does not provide any teaching of authorizing access to a network service by completing a vulnerability assessment of the workstation to identify security vulnerabilities that would compromise the secure operation of the workstation on the computer network. The Hummel reference also does not show generating workstation security credentials comprising one of integrity information describing whether the workstation has been compromised, and security posture information describing the workstation's potential for compromise, as recited in amended independent Claim 1. The workstation security credentials are generated based on the vulnerability assessment. While the Hummel reference does provide secure access to applications that can be downloadable from a network, the Hummel reference is not concerned with assessing the vulnerability of a workstation in order to control access to a network service.

In light of the differences between Claim 1 and the Dinh and Hummel references, one of ordinary skill in the art recognizes that these prior art references, alone or in combination, cannot anticipate or render obvious the recitations as set forth in amended independent Claim 1. Accordingly, reconsideration and withdrawal of the rejection of Claim 1 are respectfully requested.

Independent Claim 12

The rejection of Claim 12 is respectfully traversed. It is respectfully submitted that the Dinh and Hummel references, fail to describe, teach, or suggest the combination of (1) a local workstation assessment service, operative on the workstation, for generating workstation security credentials by completing a vulnerability assessment of the workstation to identify security vulnerabilities that would compromise the secure operation of the workstation on the computer network; (2) the workstation security credentials comprising one of integrity information describing whether the workstation has been compromised, and security posture information describing the workstation's potential for compromise; (3) a workstation security policy, operative on the workstation, for defining security policy requirements for secure operations by the workstation; (4) the local workstation assessment service further operative for comparing the workstation security credentials to the workstation security policy to determine whether the

workstation should be granted access to the network service; and (5) the local workstation assessment service further operative to authorize access to the network service by the workstation if the workstation security credentials satisfy the workstation security policy, as recited in Claim 8.

As noted above with respect to independent Claim 1, neither the Dinh reference nor the Hummel reference provide a teaching of controlling access to a network service by completing a vulnerability assessment of the workstation to identify security vulnerabilities that would compromise the secure operation of the workstation on the computer network. Further neither reference teaches workstation security credentials comprising one of integrity information describing whether the workstation has been compromised, and security posture information describing the workstation's potential for compromise, as recited in amended Claim 12.

In light of the differences between Claim 12 and the references mentioned above, one of ordinary skill in the art recognizes that the prior art references, alone or in combination, cannot anticipate or render obvious the recitations as set forth in independent Claim 12. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Independent Claim 13

The rejection of Claim 13 is respectfully traversed. It is respectfully submitted that the Dinh and Hummel references, fail to describe, teach, or suggest the combination of (1) a local workstation assessment service, operative on the workstation, for generating workstation security credentials by completing a vulnerability assessment of the workstation to identify security vulnerabilities that would compromise the secure operation of the workstation on the computer network; (2) the workstation security credentials comprising one of integrity information describing whether the workstation has been compromised, and security posture information describing the workstation's potential for compromise; and (3) a network service, operative on the network server, for determining whether the workstation should be granted access to a software service of the network service in response to receiving the workstation security credentials via the computer network, as recited in amended Claim 13.

As noted above with respect to independent Claim 1, neither the Dinh reference nor the Hummel reference provide a teaching of controlling access to a network service based on workstation security credentials comprising one of integrity information describing whether the workstation has been compromised, and security posture information describing the workstation's potential for compromise, as recited in amended Claim 13.

In light of the differences between Claim 13 and the references mentioned above, one of ordinary skill in the art recognizes that the prior art references, alone or in combination, cannot anticipate or render obvious the recitations as set forth in amended independent Claim 13. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Independent Claim 16

The rejection of Claim 16 is respectfully traversed. It is respectfully submitted that the Dinh and Hummel references, fail to describe, teach, or suggest the combination of (1) a network service operative to generate workstation security credentials by completing a vulnerability assessment of the workstation to identify security vulnerabilities that would compromise the secure operation of the workstation on the computer network; (2) the workstation security credentials comprising one of integrity information describing whether the workstation has been compromised, and security posture information describing the workstation's potential for compromise; and (3) the network service further operative to determine whether the workstation should be granted access to a software service of the network based on the workstation security credentials, as recited in amended Claim 16.

As noted above with respect to independent Claim 1, neither the Dinh reference nor the Hummel reference provide a teaching of controlling access to a software service by using workstation security credentials comprising one of integrity information describing whether the workstation has been compromised, and security posture information describing the workstation's potential for compromise, as recited in amended Claim 16.

In light of the differences between Claim 16 and the references mentioned above, one of ordinary skill in the art recognizes that the prior art references, alone or in combination, cannot anticipate or render obvious the recitations as set forth in amended independent Claim 16. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Independent Claim 19

The rejection of Claim 19 is respectfully traversed. It is respectfully submitted that the Dinh and Hummel references, fail to describe, teach, or suggest the combination of (1) issuing a request for a log-in page to a network server from a browser operating on the workstation; (2) transmitting the log-in page and an authentication plug-in from the network server to the workstation via the computer network, the authentication plug-in installable within the browser and operative to generate workstation security credentials by completing a vulnerability assessment of the workstation to identify security vulnerabilities that would compromise the secure operation of the workstation on the computer network; (3) the workstation security credentials comprising one of integrity information describing whether the workstation has been compromised, and security posture information describing the workstation's potential for compromise; (4) transmitting the workstation security credentials from the authentication plug-in to the network server via the computer network; and (5) determining at a CGI script operating on the network server whether the workstation should be granted access to a software service of the network based on the workstation security credentials, as recited in amended Claim 19.

As noted above with respect to independent Claim 1, neither the Dinh reference nor the Hummel reference provide a teaching of controlling access to a software service by using workstation security credentials comprising one of integrity information describing whether the workstation has been compromised, and security posture information describing the workstation's potential for compromise, as recited in amended Claim 19.

In light of the differences between Claim 19 and the references mentioned above, one of ordinary skill in the art recognizes that the prior art references, alone or in

combination, cannot anticipate or render obvious the recitations as set forth in amended independent Claim 19. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Independent Claim 21

The rejection of Claim 21 is respectfully traversed. It is respectfully submitted that the Dinh and Hummel references, fail to describe, teach, or suggest the combination of (1) a network assessment service operating on a network workstation assessment server on the computer network; (2) the network assessment service operative to generate workstation security credentials prior to receiving user credentials by completing a vulnerability assessment of the workstation via the computer network to identify security vulnerabilities that would compromise the secure operation of the workstation on the computer network; (3) the workstation security credentials comprising one of integrity information describing whether the workstation has been compromised, and security posture information describing the workstation's potential for compromise; (4) the network service, responsive to receiving the workstation security credentials from the network assessment service via the computer, operative to determine whether the workstation should be granted access to a software service of the network based on the workstation security credentials and the user credentials, as recited in amended Claim 21.

As noted above with respect to independent Claim 1, neither the Dinh reference nor the Hummel reference provide a teaching of controlling access to a network service with workstation security credentials comprising one of integrity information describing whether the workstation has been compromised, and security posture information describing the workstation's potential for compromise, as recited in amended Claim 21. Further, neither the Dinh nor the Hummel reference provide a teaching of network assessment service operative to generate workstation security credentials prior to receiving user credentials by completing a vulnerability assessment of the workstation via the computer network, as recited in amended Claim 21.

In light of the differences between Claim 21 and the references mentioned above, one of ordinary skill in the art recognizes that the prior art references, alone or in combination, cannot anticipate or render obvious the recitations as set forth in amended

independent Claim 21. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Independent Claim 25

The rejection of Claim 25 is respectfully traversed. It is respectfully submitted that the Dinh and Hummel references, fail to describe, teach, or suggest the combination of (1) issuing a request for a log-in page to a network server from a browser operating on the workstation; (2) transmitting the log-in page, an authentication plug-in, and a workstation policy from the network server to the workstation via the computer network, the authentication plug-in installable within the browser and operative to generate workstation security credentials by completing a vulnerability assessment of the workstation to identify security vulnerabilities that would compromise the secure operation of the workstation on the computer network; (3) the workstation security credentials comprising one of integrity information describing whether the workstation has been compromised, and security posture information describing the workstation's potential for compromise; (4) comparing the workstation security credentials to the workstation policy on the workstation to determine whether the workstation should be granted access to a software service of the network; and (5) receiving user credentials if the workstation is granted access to the software service of the network, as recited in amended Claim 25.

As noted above with respect to independent Claim 1, neither the Dinh reference nor the Hummel reference provide a teaching of granting access to a software service based on workstation security credentials comprising one of integrity information describing whether the workstation has been compromised, and security posture information describing the workstation's potential for compromise, as recited in amended Claim 25. Further, neither the Dinh nor the Hummel reference provide a teaching of receiving user credentials if the workstation is granted access to the software service of the network, as recited in amended Claim 25.

In light of the differences between Claim 25 and the references mentioned above, one of ordinary skill in the art recognizes that the prior art references, alone or in combination, cannot anticipate or render obvious the recitations as set forth in amended

independent Claim 25. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Dependent Claims 2-11, 14-15, 17-18, 20, and 22-24

The Applicants respectfully submit that the above-identified dependent claims are allowable because the independent claims from which they depend are patentable over the cited references.

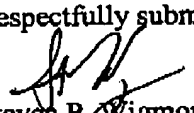
The Applicants also respectfully submit that the recitations of dependent Claims 2-11, 14-15, 17-18, 20, and 22-24 are of patentable significance. Accordingly, reconsideration and withdrawal of the rejections of the dependent claims are respectfully requested.

CONCLUSION

The foregoing is submitted as a full and complete response to the Office Action mailed on March 25, 2004. The Applicants and the undersigned thank Examiner Jackson for the consideration of these remarks. The Applicants have submitted remarks to traverse the rejections of Claims 1-25. The Applicants respectfully submit that the present application is in condition for allowance. Such Action is hereby courteously solicited.

If any issues remain that may be resolved by telephone, the Examiner is requested to call the undersigned at 404.572.2884.

Respectfully submitted,



Steven P. Wigmore
Reg. No. 40,447

King & Spalding LLP
45th Floor
191 Peachtree Street, N.E.
Atlanta, Georgia 30303
404.572.4600
K&S Docket: 05456-105004